

Web Images Videos Maps News Shopping Gmail more ▼

Scholar Preferences | Sign in

Google scholar

restoring cryptographic key IC card

Search

Advanced Scholar Search

Scholar

Articles and patents

anytime

include citations

Create email alert

Results 1 - 10 of about 2,120. (0.14 sec)

Differential power analysis

PC Kocher, *2nd edition* ... - US Patent 7,634,093, 2009 - Google Patents
 ... 51) Int. Cl. H04L 9/00 G06F 21/00 (2006.01) (2006.01) Information leaked from smart
cards and other tamper resis- tant **cryptographic** devices can be statistically analyzed
 to determine **keys** or other secret data. A data collection ...
Cited by 2,233 - *Related articles* - *Bi. Citations* - *All 20 versions*

[\[PDF\] from vulfix.co](#)**Visual cryptography for gray-level images by dithering techniques**

CC Lin, ... - Pattern Recognition Letters, 2003 - Elsevier
 ... Available online 18 October 2002. Abstract. A (k,n) -threshold visual **cryptography** scheme is
 proposed to encode a secret image into n shadow images, where any k or more of them can
 visually recover the secret image, but any $k-1$ or fewer of them gain no information about it. ...
Cited by 117 - *Related articles* - *All 8 versions*

Smart Card a Highly Reliable and Portable Security Device

L. Guillevin ... - Advances In Cryptology—CRYPTO'88, 1987 - Springer
 ... From the chip serial number, the issuer reconstructs the distribution **key** and then the computation
 result ... before sending it to the user : the external modification must then **restore** the initial ... In
 addition to these functions, when the **cryptographic** computation in the **card** reverses an ...
Cited by 18 - *Related articles* - *All 2 versions*

Checking before output may not be enough against fault-based cryptanalysis

SM Yan, ... - Computers, IEEE Transactions on, 2002 - ieeeexplore.ieee.org
 ... out that only the nAR least significant bits of d suffice to recover the entire ... 8) E. Biham and A. Shamir,
 "Differential Fault Analysis of Secret Key Cryptosystems," Proc ... and MJB Robshaw, "Comments
 on Some New Attacks on **Cryptographic** Devices," RSA Laboratories Bulletin ...
Cited by 125 - *Related articles* - *Bi. Citations* - *All 32 versions*

[\[PDF\] from geophis.com.mx](#)**IC card transporation key sei**

TP Richards, OS Examen ... - US Patent 6,230,287, 2001 - Google Patents
 ... 3/1994 (EP) 0594493 4/1994 (EP) (List continued on next page.) OTHER PUBLICATIONS
 Schneier, "Applied **Cryptography**", 1995 pp. ... **card** by retrieving using capable of supporting multiple
 applications is present on the 60 the **IC card**-s signed public **key** and verifying ...
Cited by 21 - *Related articles* - *All 4 versions*

A cryptographic key management solution for HIPAA privacy/security regulations

VB Lee, ... - Information Technology in Biomedicine, ... - 2003 - ieeeexplore.ieee.org
 ... For example, in Taiwan, the National Insurance **IC Card** is one of the major projects of the e ... (14)
 are required to recover the **key** ... V. CONCLUSIONS We have proposed a **cryptographic key**
 management solution to facilitate inter-operations among **cryptographic** mechanisms for ...
Cited by 9 - *Related articles* - *Bi. Citations* - *All 2 versions*

Cryptography and relational database management systems

J He, M Wang - Database Engineering & Applications, 2001 ... 2002 - ieeeexplore.ieee.org
 ... storage and access of confidential data in a database system When we consider inte rating
cryptographic sup-port ... The credit card number will be stored in its original plain-text form. ... For
 any plaintext m and **key** $E(k, m)$ is the ciphertext after applying encryption operation tom ...
Cited by 23 - *Related articles* - *All 11 versions*

[\[PDF\] from hp.com](#)**Key transformation unit for an IC card**

TP Richards - US Patent 6,395,723, 2002 - Google Patents
 ... on next page.) (List continued on next page.) OTHER PUBLICATIONS Schneier, "Applied
Cryptography, 2nd Edition ... to load an application from an appli- cation provider, which could be
 remote, to use an **IC card**. At least a portion of the application is encrypted using a transfer **key**. ...
Cited by 23 - *Related articles* - *All 4 versions*

Based on cryptosystem secure communication between set-top box and smart card in DTV broadcasting

TW Hou, JT Lin ... - TENCON 2007-2007 IEEE Region ... 2008 - ieeeexplore.ieee.org
 ... described the specifications of contact **IC cards** and the ISO- 10536 describes the specifications
 of contact-less **IC cards**. ... RF) signal from the channel, tuner and demodulator will process the signal
 to **restore** the TS ... 20) Simson L. Garfinkel, "Public **key cryptography**", Internet Kiosk ...
Cited by 5 - *Related articles*

[PDF] Security pitfalls in cryptography

E Schneier - EDI FORUM-DAC PARKE, 1998 - taz.newff.com
 ... once the attack is detected, the system needs to recover: generate and ... pioneered research on
 secure random number generators, differential related-key crypt- analysis ... international conferences,
 and he has broken many proposed commercial **cryptographic** algorithm, protocol ...
Cited by 28 - *Related articles* - *View as HTML* - *Bi. Citations* - *All 48 versions*

[\[PDF\] from newff.com](#)

Create email alert